Proof of Coherence: A QKD-Based Consensus Mechanism for Sustainable Post-Quantum Blockchain Systems

Sylvain Cormier
Paraxiom
sylvain@paraxiom.org

December 2025

Abstract

We present Proof of Coherence (PoC), a novel blockchain consensus mechanism that leverages real-time quantum key distribution (QKD) hardware metrics as the basis for leader election and block validation. Unlike post-quantum cryptographic approaches that defend against quantum computers using classical hardware, PoC requires nodes to operate QKD equipment and uses channel quality metrics—particularly quantum coherence time, quantum bit error rate (QBER), and visibility—as proof of physical infrastructure investment that is computationally and operationally infeasible to forge without equivalent quantum hardware. We formalize the consensus protocol, analyze its security properties under the assumption of physics-based attestation, and discuss integration with existing distributed ledger architectures. The mechanism provides Sybil resistance through hardware requirements while creating economic incentives for quantum network infrastructure development.

1 Introduction

The advent of large-scale quantum computers poses an existential threat to classical blockchain security. Current approaches fall into two categories: (1) post-quantum cryptography (PQC), which replaces vulnerable algorithms with lattice-based or hash-based alternatives, and (2) quantum key distribution (QKD), which provides information-theoretic security through physics. While PQC addresses signature and encryption vulnerabilities, it does not fundamentally change the consensus layer.

We propose Proof of Coherence, a consensus mechanism where block production rights are allocated based on demonstrated QKD channel quality. The core insight is that quantum coherence metrics—measurements that reflect the quality of quantum states in a communication channel—are computationally and operationally infeasible to spoof without actual quantum hardware and proper optical infrastructure.

1.1 Contributions

1. A formal definition of Proof of Coherence consensus based on QKD hardware metrics
2. Analysis of security properties, including Sybil resistance and attack detection
3. Protocol specification for metric collection, aggregation, and leader election
4. Integration architecture with Substrate-based blockchain frameworks

1.2 Related Work

Proof of Work (PoW) provides Sybil resistance through computational cost. Proof of Stake (PoS) and its variants (e.g., Algorand [?]) replace computation with capital lockup. Both mechanisms rely on economic assumptions rather than physical constraints.

Hardware-attested consensus has been explored through Proof of Space [?] and trusted execution environments. Our approach differs by using quantum hardware attestation, where the "proof" is a set of physics measurements that cannot be simulated classically.

The threat of quantum computers to blockchain security is well-documented [?], and various quantum-resistant approaches have been surveyed [?]. QKD integration with blockchain has been studied for key distribution [?] but not as a consensus primitive. We extend this work by making QKD channel quality the basis for leader election.

2 System Model

2.1 Network Assumptions

We consider a permissioned network of n validator nodes, each operating:

- A QKD transmitter/receiver pair (e.g., Toshiba QKD, ID Quantique)
- A hardware security module (HSM) with quantum random number generation
- Standard blockchain node software

Nodes are connected via optical fiber channels supporting QKD protocols (BB84, E91, or continuous-variable QKD). We assume partial synchrony: messages are eventually delivered within a known bound Δ.

2.2 Threat Model

We consider Byzantine adversaries controlling up to $f < n/3$ nodes. Adversaries may:

- Attempt to forge coherence metrics
- Disrupt optical channels (man-in-the-middle)
- Coordinate to maximize adversarial block production

We assume adversaries cannot violate quantum mechanical principles. Specifically, attempts to measure or clone quantum states in transit will increase QBER detectably.

3 QKD Metrics as Consensus Primitives

3.1 Hardware Metric Definitions

Each validator continuously measures the following from their QKD equipment:

Definition 1 (Quantum Bit Error Rate)**.** *The QBER $Q \in [0, 1]$ is the fraction of bits where Alice's transmitted basis matches Bob's measurement basis, but the bit values differ:*

$$Q = \frac{\textit{errors in matching bases}}{\textit{total bits in matching bases}} \tag{1}$$

A secure channel requires $Q < 0.11$ (11% threshold from BB84 security proofs).

Definition 2 (Visibility)**.** *The visibility $V \in [0, 1]$ measures interference fringe contrast in the quantum channel:*

$$V = \frac{I_{\max} - I_{\min}}{I_{\max} + I_{\min}} \tag{2}$$

where $I_{\max}$ and $I_{\min}$ are maximum and minimum detected intensities. High visibility ($V > 0.85$) indicates strong quantum correlations.

Definition 3 (Coherence Time)**.** *The coherence time τ_c characterizes the temporal stability of the quantum channel. In practical QKD systems, this manifests as the duration over which phase-encoded or polarization-encoded states remain distinguishable:*

$$\textit{Fidelity}(t) \propto e^{-t/\tau_c} \tag{3}$$

Longer coherence time indicates more stable optical paths and higher-quality quantum state transmission. For fiber-based QKD, this is influenced by thermal fluctuations, mechanical vibrations, and polarization drift.

Definition 4 (Secure Key Rate)**.** *The secure key rate R (bits/second) is the rate at which information-theoretically secure key material can be extracted:*

$$R = R_{raw} \cdot [1 - H(Q) - \chi(E)] \tag{4}$$

where $H(Q)$ is the binary entropy of the error rate and $\chi(E)$ bounds Eve's information.

3.2 Coherence Score

We define a composite coherence score C aggregating the above metrics:

Definition 5 (Coherence Score)**.** *For a validator i at time t, the coherence score is:*

$$C_i(t) = w_1 \cdot (1 - Q_i/0.11) + w_2 \cdot V_i + w_3 \cdot \frac{\tau_{c,i}}{\tau_{\max}} + w_4 \cdot \frac{R_i}{R_{\max}} \tag{5}$$

where $w_1 + w_2 + w_3 + w_4 = 1$ are configurable weights, and $\tau_{\max}$, $R_{\max}$ are normalization constants.

The score $C_i \in [0, 1]$ represents the quality of node i's quantum infrastructure relative to network standards.

4 Consensus Protocol

4.1 Protocol Overview

Proof of Coherence operates in rounds. Each round:

1. **Metric Collection**: Validators sample QKD metrics over interval δ
2. **Metric Attestation**: Metrics are signed and broadcast
3. **Score Aggregation**: Network computes coherence scores
4. **Leader Election**: Highest-scoring validator produces block
5. **Validation**: Other validators verify block and metrics

Algorithm 1 Metric Attestation Protocol

Validator i measures metrics $M_i = (Q_i, V_i, \tau_{c,i}, R_i)$
i requests attestation from k peer validators via QKD channels
for each peer $j \in \text{peers}(i)$ **do**
    j measures channel quality to i: $M_{j \to i}$
    j signs attestation: $\sigma_j = \text{Sign}_{sk_j}(M_i, M_{j \to i}, t)$
end for
i aggregates: $A_i = (M_i, \{(\sigma_j, M_{j \to i})\}_{j \in \text{peers}})$
Broadcast A_i to network

4.2 Metric Attestation

To prevent metric forgery, we employ multi-party verification:

Cross-validation ensures that a node cannot claim metrics inconsistent with what peers observe on shared channels.

4.2.1 Zero-Knowledge Metric Attestation

A critical consideration is that while QKD channels provide physics-based security for key exchange, the *reporting* of metrics occurs over classical channels. To prevent metric forgery attacks—where a node with valid QKD hardware falsifies its reported measurements—we employ zero-knowledge proofs for metric attestation.

Rather than broadcasting raw metric values (which could be fabricated), validators commit to their metrics and generate a ZK proof demonstrating:

1. The committed values satisfy coherence thresholds ($Q < 0.11$, $V > V_{\min}$, etc.)
2. The metrics are consistent with peer cross-validations
3. The proof was generated within the current epoch (preventing replay)

The implementation supports dual proof systems:

- **Groth16**: Efficient proof generation and verification for current deployments
- **STARK**: Post-quantum secure proofs ensuring long-term attestation integrity

We note that ZK proof systems introduce engineering overhead and latency; the security of PoC does not depend on ZK proofs being perfect—they serve as an additional layer of attestation integrity rather than the foundation of consensus security.

This architecture ensures that even if a malicious node possesses legitimate QKD hardware, it cannot "lie about readings" on the classical reporting channel—the ZK proof binds the attestation to actual measurements without revealing values that could be interpolated or replayed.

4.3 Leader Election

Definition 6 (Leader Election Rule)**.** *For round r, the leader ℓ_r is:*

$$\ell_r = \arg\max_{i \in \mathcal{V}} [C_i(r) + \epsilon \cdot H(r \| pk_i)] \tag{6}$$

where $\mathcal{V}$ is the validator set, H is a hash function, and $\epsilon \ll 1$ provides deterministic tiebreaking.

The leader produces a block containing:

- Transactions from the mempool

- Their attested coherence metrics A_{ℓ_r}
- Hash of previous block
- Timestamp and signature

4.4 Block Validation

Validators accept a block if:

1. The producer was the legitimate leader (highest coherence score)
2. Metric attestations are valid (correct signatures, consistent cross-validations)
3. Metrics satisfy minimum thresholds ($Q < 0.11$, $V > 0.70$, etc.)
4. Standard blockchain validity (correct parent hash, valid transactions)

5 Security Analysis

5.1 Sybil Resistance

Theorem 1 (Hardware-Based Sybil Resistance)**.** *An adversary cannot increase their probability of leader election beyond their fraction of total quantum infrastructure investment.*

Proof Sketch. Coherence score depends on physical QKD channel quality. Creating additional "virtual" validators without corresponding QKD hardware would result in:

- No attestations from peer channels (unconnected nodes score 0)
- Or sharing attestations across identities (detectable via channel uniqueness)

Thus, leader election probability is proportional to actual QKD infrastructure. □

5.2 Attack Detection via QBER

Property 1 (Eavesdropping Detection)**.** *Any attempt to intercept quantum states in transit increases QBER above the 11% threshold, triggering automatic channel rejection.*

This follows directly from quantum mechanical principles—an adversary cannot measure quantum states without disturbing them, and this disturbance manifests as increased error rates. The security bounds are well-established in the QKD literature [**?**, **?**].

5.3 Byzantine Fault Tolerance

Theorem 2 (BFT Guarantee)**.** *With $n \geq 3f + 1$ validators and coherence score verification, the protocol tolerates up to f Byzantine failures.*

The proof follows standard BFT arguments: Byzantine nodes cannot forge attestations from honest peers, and $2f + 1$ honest nodes ensure correct leader identification.

6 Implementation

6.1 Current Status

This work builds on an ongoing deployment with the KIRQ quantum network operated by Numana in Québec. Phases 0 (infrastructure setup) and 1 (QKD integration) have been completed. Phase 2 targets the consensus mechanism described in this paper.

The existing infrastructure provides:

- Operational QKD channels with real-time metric collection
- ETSI-compliant API access to hardware measurements
- HSM integration with quantum random number generation (Crypto4A)

6.2 Supporting Software Stack

Proof of Coherence is part of a production-ready post-quantum blockchain ecosystem:

QuantumHarmony. A Substrate-based blockchain with full NIST PQC integration. Current status: *3-validator testnet operational.* Cryptographic stack:

Layer	Algorithm	Standard	Purpose
Consensus (Aura)	SPHINCS+-SHAKE-256s	NIST PQC	Block signing
P2P Identity	Falcon-1024	NIST PQC	Node authentication
Key Exchange	ML-KEM-1024 (Kyber)	NIST PQC	Session establishment
Symmetric	AES-256-GCM	NIST	Message confidentiality

Multi-tier QKD identity architecture with configurable modes (`-identity-source [auto|qkd|falcon|hybr`

- Tier 1: Direct QKD hardware (Toshiba, IDQuantique, KETS, Crypto4A)
- Tier 2: QRNG entropy via PQTG gateway
- Tier 3: Software PQC fallback (Falcon-1024)

QKD Client. ETSI GS QKD 014-compliant client supporting multiple vendors (Toshiba, IDQ, Basejump). Includes Byzantine fault-tolerant consensus with zero-knowledge VRF for privacy-preserving leader election. Dual proof systems: Groth16 (efficient) and STARK (post-quantum).

PQ-QKD-Proxy / PQTG. Addresses a critical vulnerability: QKD vendors use classical TLS for management APIs, exposing quantum keys to future quantum attacks [**?**]. The proxy:

- Runs on QKD hardware (localhost isolation)
- Exposes quantum-safe API (Falcon + SPHINCS+)
- Translates to vendor's TLS API internally
- Ensures no external classical TLS exposure

QSSH. Open-source, drop-in SSH replacement published on crates.io (`cargo install qssh`). 13K SLOC Rust, MIT/Apache-2.0 licensed. Features:

- Falcon-512 key exchange, SPHINCS+ signatures
- Full SSH feature set: PTY, SFTP, port forwarding, X11, agent, multiplexing
- QKD/QRNG integration via ETSI GS QKD 014

- Double Ratchet forward secrecy
- P2P mode with NAT traversal

These components form a complete post-quantum stack; Proof of Coherence adds the consensus layer.

6.3 Architecture

We implement Proof of Coherence as a Substrate pallet, integrating with the FRAME runtime:

```
pallets/
  proof-of-coherence/
    src/
      lib.rs          # Pallet definition
      coherence.rs    # Score computation
      consensus.rs    # Leader election
      types.rs        # Metric structures
      authoring.rs    # Block production
```

6.4 QKD Hardware Integration

The system interfaces with QKD devices via the ETSI GS QKD 014 API standard:

```
GET /api/v1/keys/{slave_SAE_ID}/status
Response: {
  "source_KME_ID": "...",
  "key_size": 256,
  "stored_key_count": 42,
  "max_key_count": 1000,
  "qber": 0.023,
  "visibility": 0.94
}
```

Supported hardware includes Toshiba QKD systems, ID Quantique Clavis, and Crypto4A HSM with QRNG. The KIRQ network currently utilizes Crypto4A infrastructure for key management and entropy generation.

6.5 Performance Characteristics

Table 1: Protocol Performance

Metric	Value	Notes
Metric sampling interval	100 ms	Configurable
Attestation latency	< 50 ms	Over QKD channels
Block time	6 seconds	Substrate default
Finality	2 blocks	With GRANDPA
Message complexity	$O(n \cdot k)$	k = attestation peers

7 Economic Incentives

7.1 Infrastructure Investment

Unlike PoW (energy) or PoS (capital), PoC incentivizes:

- Deployment of QKD infrastructure
- Maintenance of high-quality optical channels
- Geographic distribution (longer channels require better equipment)

7.2 Reward Distribution

Block rewards are proportional to coherence score:

$$\text{Reward}_i = \text{BaseReward} \cdot \frac{C_i}{\sum_j C_j} \tag{7}$$

This creates continuous incentive for infrastructure improvement rather than winner-take-all dynamics.

8 Discussion

8.1 Alignment with Sustainable Blockchain Goals

The T-RIZE research agenda emphasizes sustainable, practical blockchain applications beyond cryptocurrency speculation. Proof of Coherence contributes to this vision in several ways:

1. **Energy Sustainability**: Unlike Proof of Work, PoC requires no wasteful computation. The "work" is maintaining quantum channel quality—energy goes toward useful infrastructure rather than hash puzzles. Estimated power consumption is comparable to standard networking equipment.

2. **Infrastructure Investment**: Block rewards incentivize deployment of quantum communication infrastructure, creating positive externalities beyond the blockchain itself. This aligns with public interest in quantum network development.

3. **Enterprise Applicability**: The permissioned model suits consortium deployments in supply chain, healthcare, and financial services—domains where post-quantum security is a genuine requirement.

4. **Interoperability Potential**: QKD channels between blockchain networks could enable secure cross-chain communication with information-theoretic guarantees.

8.2 Advantages

1. **Physical Attestation**: Coherence metrics are infeasible to forge without equivalent quantum hardware infrastructure

2. **Attack Transparency**: Eavesdropping attempts are immediately visible via QBER

3. **Infrastructure Development**: Creates economic incentive for quantum networks

4. **Energy Efficiency**: No wasteful computation as in PoW

8.3 Limitations

1. **Hardware Requirements**: Nodes must operate expensive QKD equipment
2. **Permissioned Setting**: Currently practical only for enterprise/consortium chains
3. **Geographic Constraints**: QKD range limited by optical fiber losses
4. **Metric Gaming**: Nodes may optimize for metrics rather than genuine channel quality. Mitigations include sliding window averages, entropy-weighted penalties for anomalous readings, and cross-link diversity requirements that make gaming economically impractical
5. **Hardware Availability**: QKD equipment remains specialized; broader adoption depends on cost reduction

8.4 Future Work

- Satellite-based QKD for global reach (e.g., integration with Micius satellite network)
- Integration with quantum repeater networks as they become available
- Hybrid PoC/PoS for public blockchain adaptation
- Formal verification of the protocol in Coq/Isabelle
- Simulation studies comparing energy consumption with PoW/PoS alternatives
- Continued deployment on KIRQ network (Phase 2 and beyond)

8.5 Research Collaboration Opportunities

This work presents several avenues for collaboration with the T-RIZE Chair:

1. **Consensus Algorithm Analysis**: Formal comparison of PoC with existing sustainable consensus mechanisms (PoS variants, PBFT, DAG-based approaches)
2. **Simulation Framework**: Development of a discrete-event simulator for PoC networks, enabling study of metric gaming, network topology effects, and failure modes
3. **Interoperability Protocols**: Design of cross-chain bridges leveraging QKD-derived trust for asset transfers between heterogeneous blockchains
4. **Application Case Studies**: Evaluation of PoC for specific use cases: biospecimen tracking, supply chain provenance, or financial settlement systems requiring post-quantum guarantees
5. **Graduate Student Projects**: Protocol implementation, security analysis, and performance benchmarking suitable for Master's or PhD research

9 Conclusion

Proof of Coherence demonstrates that quantum hardware metrics can serve as a practical basis for blockchain consensus. By tying leader election to QKD channel quality, we achieve Sybil resistance through physics rather than economics alone. The approach is immediately implementable with existing QKD hardware and provides a natural path toward quantum-secured distributed systems.

The mechanism does not claim to replace mathematical cryptography with "pure physics trust"—it uses physics measurements as one component of a rigorous protocol that still relies on digital signatures, hash functions, and standard distributed systems techniques. The novelty is in using coherence metrics as a hardware-attested proof of infrastructure investment—difficult to forge without equivalent physical resources—complementing rather than replacing traditional security mechanisms.

References

[1] E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. I. Lvovsky, and A. K. Fedorov, "Quantum-Secured Blockchain," *Quantum Science and Technology*, vol. 3, no. 3, 2018.

[2] X. Sun, P. Kulicki, and M. Sopek, "A Review of Quantum-Resistant Distributed Ledger Technologies," *IEEE Access*, vol. 11, pp. 97552–97567, 2023.

[3] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, "Quantum Computers Put Blockchain Security at Risk," *Nature*, vol. 563, pp. 465–467, 2018.

[4] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 839–894, 2022.

[5] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical Challenges in Quantum Key Distribution," *npj Quantum Information*, vol. 2, 16025, 2016.

[6] Y.-A. Chen et al., "An Integrated Space-to-Ground Quantum Communication Network over 4,600 Kilometres," *Nature*, vol. 589, pp. 214–219, 2021.

[7] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling Byzantine Agreements for Cryptocurrencies," in *Proc. 26th Symposium on Operating Systems Principles (SOSP)*, pp. 51–68, 2017.

[8] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," in *Proc. 3rd Symposium on Operating Systems Design and Implementation (OSDI)*, pp. 173–186, 1999.

[9] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of Space," in *Advances in Cryptology – CRYPTO 2015*, pp. 585–605, Springer, 2015.

[10] ETSI, "Quantum Key Distribution (QKD); Application Interface," ETSI GS QKD 014 V1.1.1, 2019.

[11] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The Security of Practical Quantum Key Distribution," *Reviews of Modern Physics*, vol. 81, no. 3, pp. 1301–1350, 2009.

[12] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure Quantum Key Distribution with Realistic Devices," *Reviews of Modern Physics*, vol. 92, no. 2, 025002, 2020.

[13] S. Cormier, "Residual Classical Vulnerabilities in Quantum Key Distribution Control Channels," *Cryptology ePrint Archive*, Paper 2025/106693, 2025.